CLAIMS

What we claim is:

1. A method for authentication in a public cryptographic system comprising:

creating a first private key and corresponding first public key;

creating a second private key associated with the first private key and creating a second public key corresponding to the second private key;

outputting the second private key once such that it can be re-created;

outputting the second public key when outputting the first public key; and

using the first private key for authentication.

2. The method of claim 1, wherein outputting the second public key comprises:

creating at least two shares of the second public key; and

outputting each share once to a different entity.

3. The method of claim 1, further comprising:

re-creating the second private key; and

using the second private key for authentication.

4. The method of claim 3, further comprising:

disabling the first private key when the second private key is used for authentication

5. The method of claim 3, further comprising:

creating a third private key associated with the second private key and creating a third public key corresponding to the third private key; and

outputting the third public key.

6. The method of claim 5, further comprising:

outputting the third private key once such that it can be re-created; and

re-creating the third private key and using the third private key for authentication.

7. The method of claim 5, further comprising:

disabling use of the second private key for authentication;

using the third private key for authentication; and

re-creating the second private key and using the second private key for authentication.

8. The method of claim 3, further comprising:

creating a third private key associated with the second key and creating a third public key corresponding to the third private key;

creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key;

outputting the fourth private key once such that it can be re-created; and

outputting the third and fourth public keys.

9. The method of claim 8, further comprising:

disabling use of the second private key for authentication; and

using the third private key for authentication.

10. The method of claim 9, further comprising:

re-creating the fourth private key; and

using the fourth private for authentication.

11. A method for verification in a public cryptographic system comprising:

receiving a first public key;

receiving a second public key associated with the first public key;

using the first public key for authentication; and

using the second public key for authentication if the first public key fails.

12. The method of claim 11, further comprising:

receiving a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

13. The method of claim 11, further comprising:

receiving a third public key and a fourth public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

14. Apparatus for authentication in a public cryptographic system comprising:

means for creating a first private key and corresponding first public key;

means for creating a second private key associated with the first private key and creating a second public key corresponding to the second private key;

means for outputting the second private key once such that it can be re-created;

means for outputting the second public key when outputting the first public key; and

means for using the first private key for authentication.

15. The apparatus of claim 14, wherein means for outputting the second public key comprises:

means for creating at least two shares of the second public key; and

means for outputting each share once to a different entity.

16. The apparatus of claim 14, further comprising:

means for re-creating the second private key; and

means for using the second private key for authentication.

17. The apparatus of claim 16, further comprising:

means for creating a third private key associated with the second private key and creating a third public key corresponding to the third private key; and

means for outputting the third public key.

18. The apparatus of claim 16, further comprising:

means for creating a third private key associated with the second key and creating a third public key corresponding to the third private key;

means for creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key;

means for outputting the fourth private key once such that it can be re-created; and

means for outputting the third and fourth public keys.

19. Apparatus for verification in a public cryptographic system comprising:

means for receiving a first public key;

means for receiving a second public key associated with the first public key;

means for using the first public key for authentication; and

means for using the second public key for authentication if the first public key fails.

20. The apparatus of claim 19, further comprising:

means for receiving a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

21. The apparatus of claim 19, further comprising:

means for receiving a third public key and a fourth public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

22. A machine readable medium in a public cryptographic system comprising:

a set of code segments for creating a first private key and corresponding first public key;

a set of code segments for creating a second private key associated with the first private key and creating a second public key corresponding to the second private key;

a set of code segments for outputting the second private key once such that it can be re-created;

a set of code segments for outputting the second public key when outputting the first public key; and

a set of code segments for using the first private key for authentication.

23. The medium of claim 22, wherein the set of code segments for outputting the second public key comprises:

code segments for creating at least two shares of the second public key; and

code segments for outputting each share once to a different entity.

24. The medium of claim 22, further comprising:

a set of code segments for re-creating the second private key; and

a set of code segments for using the second private key for authentication.

25. The medium of claim 24, further comprising:

a set of code segments for disabling the first private key by using the second private key for authentication

26. A machine readable medium in a public cryptographic system comprising:

a set of code segments for receiving a first public key;

a set of code segments for receiving a second public key associated with the first public key;

a set of code segments for using the first public key for authentication; and

a set of code segments for using the second public key for authentication if the first public key fails.

27. The medium of claim 26, further comprising:

a set of code segments for receiving a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

28. The medium of claim 26, further comprising:

a set of code segments for receiving a third public key and a fourth public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

29. A method for authentication in a public cryptographic system comprising:

creating a private key and corresponding public key with associated system parameter;

outputting the system parameter when outputting the public key; and

using the private key for authentication.

30. The method of claim 29, further comprising:

creating a new private key using a previous private key and the system parameter; and

using the new private key for authentication.

31. The method of claim 29, further comprising:

creating a counter value indicating the generation of public and private keys; and

outputting the counter value when outputting the public key.

32. The method of claim 31, further comprising:

creating the new private key using a previous private key and the system parameter based on the counter value; and

using the new private key for authentication.

33. A method for verification in a public cryptographic system comprising:

receiving a public key;

receiving a system parameter associated with the public key;

authenticating using the public key; and

generating a new public key and authenticating using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

34. The method of claim 33, wherein generating the new public key comprises:

using a number of powers of the previous public key for authentication; and

accepting one that works as the new public key.

35. The method of claim 33, further comprising

receiving a counter value indicating the generation of private and public keys; and

generating the new public key using the previous public key and the system parameter based on the counter value.

36. Apparatus for authentication in a public cryptographic system comprising:

means for creating a private key and corresponding public key with associated system parameter;

means for outputting the system parameter when outputting the public key; and

means for using the private key for authentication.

37. The apparatus of claim 36, further comprising:

means for creating a new private key using a previous private key and the system parameter.

38. The apparatus of claim 36, further comprising:

means for creating a counter value indicating the generation of public and private keys; and

means for outputting the counter value when outputting the public key.

39. The apparatus of claim 38, further comprising:

means for creating a new private key using a previous private key and the system parameter based on the counter value.

40. Apparatus for verification in a public cryptographic system comprising:

means for receiving a public key;

means for receiving a system parameter associated with the public key;

means for authenticating using the public key; and

means for generating a new public key and authenticating using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

41. The apparatus of claim 40, wherein generating the new public key comprises:

means for using a number of powers of the previous public key for authentication; and

means for accepting one that works as the new public key.

42. The apparatus of claim 40, further comprising

means for receiving a counter value indicating the generation of private and public keys; and

means for generating the new public key using the previous public key and the system parameter based on the counter value.

43. A machine readable medium in a public cryptographic system comprising:

a set of code segments for creating a private key and corresponding public key with associated system parameter;

a set of code segments for outputting the system parameter when outputting the public key; and

a set of code segments for using the private key for authentication.

44. The medium of claim 43, further comprising:

a set of code segments for creating a new private key using a previous private key and the system parameter.

45. The medium of claim 43, further comprising:

a set of code segments for creating a counter value indicating the generation of public and private keys; and

a set of code segments for outputting the counter value when outputting the public key.

46. The medium of claim 45, further comprising:

a set of code segments for creating a new private key using a previous private key and the system parameter based on the counter value, if the previous private key is not active.

47. A machine readable medium in a public cryptographic system comprising:

a set of code segments for receiving a public key;

a set of code segments for receiving a system parameter associated with the public key;

a set of code segments for authenticating using the public key;

a set of code segments for generating a new public key and authenticating using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

48. The medium of claim 47, wherein the set of code segments for generating the new public key comprises:

code segments for using a number of powers of the previous public key for authentication; and

code segments for accepting one that works as the new public key.

49. The medium of claim 47, further comprising

a set of code segments for receiving a counter value indicating the generation of private and public keys; and

a set of code segments for generating the new public key using the previous public key and the system parameter based on the counter value.